REMARKS/ARGUMENTS

Sections 3-4 and 7-9 of the Office Action raise objections that the description and claims are not in a form preferred in US practice, and the description and claims have been amended to seek to conform to US practice to overcome these objections.

Sections 10 to 19 of the Office Action reject all claims 1 to 8 under 35 USC § 102(e) as being anticipated by Publication No. 2004/0111531 to Staniford et at (Staniford).

We submit that Staniford discloses detection of a worm in a computer network and discarding or rerouting messages from a network found to contain a worm to reduce the spread of the worm (abstract, [0006], [0008], [0010]). A "whitelist" is maintained of characteristics that are used to determine whether a worm screen will allow a message to be transmitted via a network. The whitelist may include a list of addressees to whom messages may be sent ([0013]). In a first embodiment, a worm screen examines messages issued by a system and discards messages to be sent to addresses not included in a whitelist ([0035]). In a second embodiment, a worm detector determines whether a message is sent by a system to an address rarely used by that system and if so registers the occurrence as an anomaly ([0036]). In one embodiment, a traffic whitelist of, for example traffic between two endpoints which have communicated recently may be dynamically maintained and edited ([0082] – [0086]). We therefore submit that there is no hint or suggestion in Staniford of capturing an outgoing email and updating a whitelist with the intended recipient in order to filter incoming emails to allow back into the system -without further analysis - only emails from addresses to which emails have been sent, as indicated by the whitelist, as claimed in claims 1 and 5. On the contrary, outgoing messages are captured in Staniford only to determine whether the addressees are already on a whitelist and allowing transmission of the message only if the addressees are on the

whitelist. Staniford therefore teaches away from updating a whitelist with addressees of outgoing messages, since doing so would completely invalidate the system proposed in Staniford by allowing all emails to be transmitted. We therefore submit that claim 1, and 5, and therefore the claims dependent on 1 and 5 respectively are novel and inventive in the light of Staniford.

Sections 20 to 28 of the Office Action reject all claims 1 to 8 under 35 USC § 102(a) as being anticipated by MajorNewswire.com, "Red Earth Software Releases Policy Patrol version 2.0" (MajorNewswire).

We submit that MajorNewswire discloses "adding email addresses to filters" (page 1 paragraph 3) and "email filtering" and "filtering on email addresses" (page 1 paragraph 4). We therefore submit that there is not the slightest hint or suggestion in MajorNewswire of capturing an outgoing email and updating a whitelist with the intended recipient in order to filter incoming emails to allow back into the system - without further analysis - only emails from addresses to which emails have been sent as indicated by the whitelist, as claimed in claims 1 and 5. We therefore submit that claim 1, and 5, and therefore the claims dependent on 1 and 5 respectively are novel and inventive in the light of MajorNewswire.

Sections 29 to 37 of the Office Action reject all claims 1 to 8 under 35 USC § 102(a) as being anticipated by www.Randomhacks.net, "Bayesian Whitelisting: Finding the Good Main Among the Spam" (Randomhacks).

We submit that Randomhacks discloses an "automatic whitelisting" system (page 1 paragraph 1). However, the teaching appears to be to determine whether incoming messages are spam messages dependent on the addresses in the email address (page 3 second full paragraph) and to add the sender's name to the whitelist if the incoming message has a low probability of being a spam message (page 1 paragraph 5; page 2

second complete paragraph; page 4 lines 1-2). We therefore submit that there is not the slightest hint or suggestion in Randomhacks of capturing an outgoing email and updating a whitelist with the intended recipient in order to filter incoming emails to allow back into the system - without further analysis - only emails from addresses to which emails have been sent as indicated by the whitelist, as claimed in claims 1 and 5. We therefore submit that claim 1, and 5, and therefore the claims dependent on 1 and 5 respectively are novel and inventive in the light of Randomhacks.

Sections 38 to 46 of the Office Action reject all claims 1 to 8 under 35 USC § 102(a) as being anticipated by www.rhyolite.com, "Automatic white-listing from outgoing email" (Rhyolite).

We submit that Rhyolite teaches against the use of outgoing email addresses to generate a whitelist for accepting incoming emails for two reasons. First, that replies to an email may come from a different email address at a same organisation from the email address to which an original email was sent (page 1 text lines 6-9). Second, because some users reply to spam messages and therefore the spam address would inappropriately be added to the whitelist (page 1 text lines 15-22). Rhyolite appears to teach that to overcome this problem it would also be necessary to date the additions to the whitelist and delete entries older than 90 days optionally including vetting the whitelist against addresses of incoming emails (page 1 last paragraph). It is not clear how it is determined whether the incoming emails were spam and therefore how the vetting occurs. We therefore submit that Rhyolite teaches away from capturing an outgoing email and updating a whitelist with the intended recipient in order to filter incoming emails to allow back into the system - without further analysis - only emails from addresses to which emails have been sent as indicated by the whitelist, as claimed in claims 1 and 5. We therefore submit that claim 1, and 5, and therefore the claims dependent on 1 and 5 respectively are novel and inventive in the light of Rhyolite.

Sections 47 to 55 of the Office Action reject all claims 1 to 8 under 35 USC § 102(a) as being anticipated by www.hexamail.com, "Hexamail" (Hexamail).

It will be noted that the Hexamail reference cited is actually four documents which have been cobbled together by the Examiner, pages of which have been numbered 1-8 by the Examiner, and we use these page numbers below.

We submit that Hexamail discloses analyzing each [e]mail received and sent by an organization (Hexamail page 3 paragraph 1). Only incoming email from the Internet to a server is filtered (page 5 paragraph 6). We therefore submit that there is not the slightest hint or suggestion in Hexamail of capturing an outgoing email and updating a whitelist with the intended recipient in order to filter incoming emails to allow back into the system - without further analysis - only emails from addresses to which emails have been sent as indicated by the whitelist, as claimed in claims 1 and 5. We therefore submit that claims 1 and 5, and therefore the claims dependent on 1 and 5 respectively, are novel and inventive in the light of Hexamail.

We have sought to comment on the Office Action rejections at face value. However, on reviewing the Office Action it appears to us that in respect of the first citation Staniford the Examiner has merely recited the words of the claims and stated baldly that they are disclosed by Staniford in "e.g. col. 7". Since Staniford is not numbered by columns, a charitable interpretation is that the Examiner intended "e.g. page 7". We submit that this is unsatisfactory without any discussion of what Staniford actually discloses. In respect of the remaining citations, the Examiner appears merely to have cut and pasted the rejection based on Sandi ford for each of the other citations and merely replaced "Sandi ford" by the name of the citation and replaced "e.g. col. 7" by "e.g. pages 1,2" irrespective of what page numbers actually exist in the respective citations. It may be that the Examiner performed the cut and paste with the intention of then amending the rejection in respect of each citation in terms of what is actually

disclosed in each citation, but somehow the Office Action was released before the Examiner completed that analysis.

CONCLUSION

For at least the reasons set forth above, reconsideration and allowance of this application are believed to be in order, and such action is hereby solicited. If any points remain an issue which the Examiner feels may be best resolved through a telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below. The Examiner is invited and encouraged to telephone the undersigned with any concerns in furtherance of the prosecution of the present application.

Please charge any deficiency as well as any other fee(s) which may become due at any time during the pendency of this application, or credit any overpayment of such fee(s) to Deposit Account No. 50-2896.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

November 26, 2007
Dated:

Joseph P. Quinn (Reg. No. 45,029)
Customer No. 71130
Attorney for Applicant(s)
SEYFARTH SHAW LLP
World Trade Center East
Two Seaport Lane, Suite 300
Boston, MA 02210
Tel: 617-946-4833
Fax: 617 946-4801
E-mail: bosippto@seyfarth.com